Grow | **Protect** | **Operate** | Finance

大成 DENTONS

Modernizing Québec privacy law

Protecting and defending your organization

February 15, 2022 | 1:15 p.m. – 2:15 p.m. ET

Agenda

1. Our objectives
2. Our previous webinar on modernizing privacy law: your questions answered
3. Protecting your organization – Prevention
4. Protecting your organization – Remedies
5. Key Lessons

Our objectives

Supporting you in managing compliance

- Spotlight on:
  - **new** obligations and **organizational** consequences
  - their relevance for the protection of the company
- Difference between:
  - Prevention: Highlights of organizational transformations required to demonstrate compliance
  - The remedies: Description of the enforcement mechanism and remedies available to businesses
- But before: Some answers to your questions

Our previous webinar

Answers to your questions

Scope of the application of Act 25

Does it apply to banks under federal jurisdiction?

- No, but …
- Constitutional debate: Legislative jurisdiction over the protection of personal information (PI) in the private sector according to the constitutional laws of Canada:
  - Federal jurisdiction, according to article 91.2 on the "Regulation of trade and commerce"? OR
  - Provincial jurisdiction, according to article 92.13 on "Property and civil rights in the province"?
- Banks are “federal works, undertakings or businesses”
  - According to section 91.15: “Banks, Incorporation of Banks and Issuance of Paper Money”
  - According to 4.1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA): it applies to the PI of consumers and employees of any "federal undertaking", BUT
- According to Act 25, section 1, it applies to any “business”, that is, “the carrying on of an organized economic activity by one or more persons”.
- The *Commission d’accès à l’information* (CAI) regularly exercised jurisdiction over federal banks

Scope of the application of Act 25

What considerations apply to other province regulators in the management of people's personal information in Québec?

- Public Sector Legislation
- Other provincial and federal regulators are subject to their provincial or federal freedom of information and protection of privacy laws in the public sector
- These laws apply regardless of the origin of the individual to whom the PI relates

Fines and Penalties

Are there penalties and fines for the breaches resulting from malicious actors or virus?

- No
- Companies have an obligation to apply the necessary safeguards based on the risk and sensitivity of the PI
- The administration of a penalty or fine will result from any breach of this obligation, regardless of the cause of the violation

Service providers

Are there any specific obligations which apply to service providers?

- Not in the act, but in fact:
  - The law applies to PI sent to a third party such as a service provider (section 1)
  - The third party must ensure:
    - The protection of the PI which is entrusted at a level equivalent to that imposed on its customer
    - The use of PI exclusively for consistent purposes
    - Compliance with contractual obligations for the protection of PI under the service agreement

Not-for-profit organizations

Does Act 25 apply to non-profit organizations?

- It depends
  - If the organization is engaged in a business activity, YES
  - If not, the obligations of the organization in terms of protection of PI falls under articles 35 at 40 of the Civil Code:
    - Collection, use and disclosure of personal information subject to consent or to authorization by law
    - Use can only be for consistent purposes
    - PI errors need to be corrected and the individual may have access to it, unless prohibited

➢ Violation of privacy rights is the object of a right of action

Transfers outside of Québec

How will the Province treat cross-border transfers under the new regime, particularly with respect to financial transactions to the United States and other countries not having equivalent legislation?

- Will require a formal privacy impact assessment (PIA)

- The new regime:
  - The company must carry out a PIA to ensure "adequate safeguards" depending on the destination

- The current regime:
  - The company cannot communicate the PI outside of Québec unless "taking all reasonable means to ensure that the information will not be used for irrelevant purposes or communicated to third parties without the consent of the persons concerned"

➢ Any PI from a European country cannot be transferred out of Canada without authorization, such as the transfer allowed under the standard contractual clauses approved by the European Commission

Organization transformation

Since certain provisions come into force on September 22, 2022, when must companies start updating their privacy policies?

- Now!

  ➢ **Our guide:**

  Bill 64: Québec is modernizing its privacy legislation: A practical guide

  https://www.dentons.com/en-ca/insights/guides-reports-and-whitepapers/2021/october/29/bill-64-on-modernizing-quebec-privacy-law-a-practical-guide

Main differences between the new Québec Act 25 and other Canadian laws

- Increased consent and transparency requirements *
- Clarification of the concept of "de-identified information" and of "anonymized information"
- Right to portability/mobility *
- Obligation to carry out privacy impact assessments (PIAs) in certain circumstances, including the transfer of PI out of Québec
- Mandatory parental consent for minors Under 14
- Right to "deindexation"
- Financial penalties administered by regulator *

* Also proposed in former Bill C-11 seeking to amend the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Protecting your organization

Prevention

1. The key word: due diligence

(in force 22.9.2022)

- A governance structure to ensure and demonstrate compliance: Sections 3.1 and 3.2
  - The person with the highest authority ensures that the law is respected and enforced
  - He or she may delegate this function in writing, in whole or in part
  - Title and contact information of the privacy officer is published
  - The company must establish and implement policies and practices governing its governance with respect to privacy, including:
    - Processing methods and measures to protect personal information
    - The framework applicable to the retention and destruction of such information
    - Assignment of roles and responsibilities of staff
    - Establishing a privacy complaint process

➢ Proportionate to the nature and importance of the company's activities

➢ Approved by the Privacy Officer

1. Keyword: due diligence (continued)

(in force 22.9.2022)

- A Security Incident Response Plan (Section 3.5) for:
  - Being alerted as soon as possible that a confidentiality incident has occurred
  - Taking reasonable steps to reduce the risk of harm and prevent new incidents of the same nature from occurring
  - Determining if the incident poses a risk of serious harm
  - If yes, notify:
    - the Commission d'accès à l'information (CAI)
    - any individual affected
    - any organization able to reduce the risk

1. Keyword: due diligence (continued)

(in force in 2023)

- A privacy impact assessment (PIA) development process (Section 3.3)
  - Applicable to any project to acquire, develop and redesign an information system or electronic service delivery involving the collection, use, disclosure, retention or destruction of PI.
  - Subject to consultation with the privacy officer at the outset of the project
  - Proportionate to the sensitivity of the information concerned, the purpose of its use, its quantity, its distribution and its medium.

- A PIA for personal information transfers outside of Québec (Article 17)

2. Enhancing the Terms of Consent

(effective in 2023)

- (Section 4.1): Develop consent mechanisms for minors
  - Less than 14 years: consent of parent or guardian
  - Between 14 and 18: consent by minor, parental authority or guardian
- (Section 14): Obtain specific consent for each purpose
  - Asked for each purpose, in simple and clear terms
  - Separate disclosure of all other information
- (Section 22): Highlight the right to withdraw consent

3. Improving Transparency

- Update privacy policies under section 7

- (Section 8.1) Describe the use of technology
  - Describe any technology that includes functions to identify, locate or profile, such as the use of certain targeting technologies
  - Highlight the means available to activate these functions

- (Article 12.1) Declare automated mechanisms
  - Report the use of PI to make a decision based exclusively on automated processing by the time the decision is communicated to the person.

4. New individual rights response mechanisms and guidelines

- (Section 12.1): Rights relating to automated decisions:
  - Access to the PI used to make the decision and the reasons, key factors and parameters that led to the decision
  - Rectification of the PI used to make the decision
  - Submissions to a company employee who can review the decision

- (Section 28.1): Right to "forget"
  - Cessation of dissemination or deindexation

- (Section 28): Right to have the PI communicated to another body (Right to mobility/portability)
  - The PI collected from the applicant, and which has not been created or inferred by the organization, must be communicated in a structured and commonly used format.

➢ Each of these rights is subject to conditions that must be the object of guidelines

Protecting your organization
Remedies

Applications for authorization

- (Section 46) Abusive Claims
  - A company may ask the Commisison d’accès à l’information (CAI) for authorization to disregard requests that are manifestly abusive:
    - By their number,
    - By their repetitive or systematic nature
    - Because they don't comply with the purpose of the law
- A company may request the CAI to limit the request or extend response time
- The company can assert to the CAI that the request is frivolous or made in bad faith so that it refuses to process it

Contestation a request for rectification

- (Section 53)
- The company can prove that PI does not need to be rectified unless it was communicated to the company by or with the agreement of the individual.

Appeal and contestation

- (Section 61)
  - Appeal
    - of a final decision of the CAI before a judge of the Court of Québec, on any question of law or jurisdiction
    - of an interlocutory decision with leave of a judge
- Contestation
  - A company may also challenge an order made by the CAI's surveillance division before a judge of the Court of Quebec.

Submissions

- (Section 90.4)
- Before an administrative monetary penalty can be imposed, the company must:
  - have been notified and
  - have the opportunity to present their observations and produce any document to complete their file.

➢ Hence the importance of the governance structure and internal policies to demonstrate compliance

Request reconsideration

- (Section 90.6)
- The company may, in writing, request the CAI to reconsider the decision to impose an administrative monetary penalty within 30 days of notification of the notice of claim.

Defences

- (Section 92.3). In determining a sentence, a judge shall consider the following factors, among others:
- the nature, seriousness, repetitiveness and duration of the offence: **The company could invoke the uniqueness of the breach and its efforts to remedy it as soon as possible, for example with a Security Incident Response Plan and a report that documents its response in detail according to a well-established template.**
- whether the company was negligent or reckless: **The company could present the documentation of its due diligence**
- the foreseeable nature of the offence or the failure to act on recommendations or warnings to prevent it: **The company could submit its security plan to argue that it is adequate according to the risk assessment**
- attempts to conceal the offence or failure to attempt to mitigate the consequences of the offence: **The company should be able to demonstrate that it has been transparent**
- the number of persons involved in the offence and the risk of harm to those persons: **By reacting quickly to an incident, the business can mitigate the risk of harm.**

Key lessons on compliance

1. The best protection is proof of due diligence.

2. Due diligence is demonstrated with a clear and effective governance structure, as well as comprehensive and specific internal policies.

3. "There's no point running, you have to start on time"; these measures need to be developed now to be adopted in time.

4. Planning for the compliance exercise should be based on a gap analysis and a risk analysis for each gap.

5. Compliance must be documented to be demonstrated.

大成 DENTONS

Thank you

Chantal Bernier
Lead of the National Privacy and Cybersecurity practice group, Ottawa
+ 1 613 783 9684
chantal.bernier@dentons.com

Alexandra Quigley
Senior Associate, Montréal
+ 1 514 878 5856
alexandra.quigley@dentons.com